POLICY 1325.00 Information Technology Security Awareness
Issued April 12, 2007

SUBJECT: Policy for Information Technology Security Awareness

APPLICATION: This policy is intended for statewide compliance and applies to all Executive Branch Departments, Agencies, Trusted Partners, Boards or Commissions using State information network and IT resources.

PURPOSE: This policy establishes a statewide policy for the purpose of security awareness and training and to inform all levels of State's personnel of the importance of the information they handle and the legal and business reasons for maintaining confidentiality, availability and integrity. All employees must understand the need for security, the specific security related requirements expected of them, and the consequences of noncompliance.

CONTACT AGENCY: Michigan Department of Information Technology (MDIT)
Office of Enterprise Security

TELEPHONE: 517/241-4090

FAX: 517/241-2013

SUMMARY: This policy will address two major security awareness components:

Awareness (What): identify and implement programs and products designed to convey general security information to State of Michigan (SOM) users. Such activities include, but are not limited to, a statewide information security awareness training program, generating security literature and promoting good security through security web sites and newsletters.

Training (How): identify and implement security training programs more specific to the user role (i.e. project manager, system administrator, security liaison, etc.) with in the agency. This will provide the users with training applicable to their level of responsibility.

PROCEDURE:

It is the Agency/Department who gathers data, enters it into the system, verifies its accuracy, specifies the purposes to which it can or will be used, designates who can use it, and ultimately, fills a business need for its use.

- Agency responsibility as Data Owners:
  - Each Agency Director within their area of responsibility shall ensure:
    a. The appointment of a security awareness coordinator who will serve as liaison to the Department of Information Technology security awareness coordinator.
    b. All SOM employees and trusted partners complete the SOM Information Security Awareness training prior to accessing the SOM Network and IT resources.
    c. All SOM employees and trusted partners handle information for which they are responsible in a manner in accordance with this and all SOM policies.
    d. SOM employees and trusted partners are trained to ensure they are aware of their role in protecting SOM information and data, as set forth in this policy.
    e. Internal agency security polices and procedures are implemented, maintained and enforced that compliment and comply with this policy.

f. Employees are advised of the necessity of complying with DIT policies and laws pertaining to the protection of State of Michigan Information, because non-compliance may leave the State liable and employees vulnerable to prosecution and civil suit, as well as disciplinary action.

- Agency responsibility as Data Custodians:

  - Agency Directors in conjunction with the Department of Information Technology, Chief Information Security Officer (CISO) shall ensure:

    a. A structured SOM security awareness program is formulated and maintained to ensure that SOM employees and trusted partners who require access to the State's information in the conduct of official business are familiar with their responsibilities for protecting such information from unauthorized disclosure.
    b. All agencies implement security awareness workshops for Agency security awareness coordinators.

  - The Department of Information Technology, CISO shall ensure:

    a. A security awareness coordinator is appointed to develop and implement an enterprise security awareness program.

Terms and Definitions

Agencies	Is the principal department of state government as created by Executive Organization Act 380 of 1965.
Availability	Ensuring timely and reliable access to and use of information and assuring that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them.
Business Owner	Responsible for administration of systems is usually the owner of the primary business functions served by the application, the application's largest stakeholder.
Confidentiality	Protecting information from unauthorized disclosure or interception and assuring that information is shared only among authorized persons and organizations.
Data Custodian	The individual or organization that has responsibility delegated by the data owner for maintenance and technological management of their data and systems.
Data/Information	Is SOM Agency information. No distinctions between the words data and information are made for purposes of this policy.
Data Owner	Usually a member of senior management of an organization and is ultimately responsible for ensuring the protection and use of the data.
Due Care	Shows that an organization has taken responsibility for the activities that take place within the organization and has taken the necessary steps to help protect the SOM, its resources and employees from possible risk.
Due Diligence	Is the practice by implementing controls and safeguards that make sure that the protection mechanisms are continually maintained and operational.
Information Technology Resources	Computers, storage peripherals, network equipment and wiring, network-attached printers and fax machines.
Integrity	Guarding against improper information modification and/or destruction, ensuring information has not been altered by unauthorized people and the assurance that the information can be relied upon to be sufficiently accurate for its purpose.
Trusted Partner	Is a person (i.e. vendor, contractor, 3rd party, etc.) or entity that has contracted with the State of Michigan to perform a certain service or provide a certain product in exchange for valuable consideration, monetary, or goods and services.

- **Authority**

  This policy obtains its authority from “1305.00 Enterprise Information Technology Policy”.

- **Enforcement**

  All enforcement for this policy shall be in compliance with 1305.00 Enterprise Information Technology Policy.

- **Developing Standards and Procedures for this Policy**

  All requirements for developing standards and procedures for this policy shall be in compliance with the 1305.00 Enterprise Information Technology Policy.

- **Exceptions**

  All exception requests to this policy must be processed in compliance with 1305.00 Enterprise Information Technology Policy.

- **Effective Date**

  This policy will be effective immediately upon release.

* * *